What Is Claimed Is:

1   1.   A method of declaring an incident in an enterprise

2 comprising:

3   providing a number of alert indications containing

4 information concerning an incident related to the enterprise; and

5 either

6   comparing one or more of the alert indications to a set of

7 rules, and if a match occurs between the set of rules, and the

8 alert indication, declaring an incident based on the match, or

9   comparing one or more of the alert indications to a decision

10 table containing a number of defined alert events; remembering

11 each alert indication that matches one of the defined alert

12 events, comparing the remembered alert indication to correlation

13 data in the decision table, and if a match occurs between the

14 remembered alert indication and the correlation data, declaring

15 an incident based on the match; or

16   if no match occurs between the alert indication and the

17 correlation data or the rules set, declare an incident if the

18 alert indication meets a defined default threshold value.

1   2.   The method of claim 1, wherein the defined default

2 threshold value is a level of severity in the alert indication.

1   3.   The method of claim 1, further comprising displaying an

2 incident ticket for each incident declared, the incident ticket

35

3 including a description of the incident, a conclusion based on

4 incident description, any actions responsive to the conclusion,

5 one or more incident tracking rules which identify one or more

6 further alert indications for association with the incident

7 ticket, and a detail of the alert indications associated with the

8 incident.

1   4.   The method of claim 1, further comprising the step of

2 tracking further alert indications once an incident ticket is

3 declared and associating the further alert indications with the

4 incident ticket based on one or more incident tracking rules.

1   5.   The method of claim 4, wherein the associating step is

2 performed only if the further alert indications pass a threshold

3 value or table lookup from a user-editable table which lists

4 enterprise policy attributes associated with particular alert

5 codes, categories, or threat characterizations.

1   6.   The method of claim 4, further comprising updating the

2 incident tracking rules based on one or more further alert

3 indications.

1   7.   The method of claim 1, wherein the alert indications

2 include information having a common format.

1   8.   The method of claim 1, wherein the enterprise is a

2   network with a number of network devices that supply the alert

3   indications for incident declaration.

1   9.   The method of claim 1, wherein the default defined

2   value derives from a set of rules defining default conditions for

3   declaring an incident.

1   10.   A system for declaring an incident in an enterprise

2   comprising:

3   a) a decision table containing a number of defined alert

4   events, and a set of correlation data that identifies patterns in

5   alert indications inputted to the decision table, the decision

6   table remembering inputted alert indications matching defined

7   alert events, and declaring an incident if a match occurs between

8   remembered alert indications and the correlated data;

9   a set of rules containing a number of query statements,

10   wherein a match between at least one of the rules and the

11   inputted alert indications result in an incident declaration; and

12   a set of default standards specifying a minimum value to

13   declare an incident should a match not occur with the decision

14   tables or set of rules.

1   11.   The system of claim 10, further comprising a display of

2   the incident as an incident ticket, the incident ticket including

3   a description of the incident, a conclusion based on incident

4 description, any actions responsive to the conclusion, one or

5 more incident tracking rules which identify one or more further

6 alert indications for association with the incident ticket, a

7 detail of the alert indications associated with the incident,

8 followed by a listing of "raw events" that, if requested by the

9 user, contains information that has been left in the native or

10 vendor-specific format of the original sensor that produced the

11 event.

1   12. The system of claim 10, further comprising an alert

2 processing system that tracks inputted alert indications, filters

3 out inputted alert indications that do not meet a threshold

4 value, compares the inputted information to a tracking rule to

5 determine whether the inputted information should be associated

6 with a declared incident.

1   13. The system of claim 10, further comprising a database

2 for storing at least the declared incidents.

1   14. The system of claim 12, further comprising a database

2 for storing at least the declared incidents and alert indications

3 passing the threshold value.

1   15. The system of claim 13, further comprising a web

2 server, linking the system to one or more users via a global

3 network.

1   16. The system of claim 10, further comprising means for

2   displaying the declared incident.

1   17. The system of claim 10, wherein the rules are a

2   combination of default rules and customized rules.

1   18. The system of claim 10, wherein the enterprise is a

2   network and the inputted information is supplied by a number of

3   network devices.

1   19. The system of claim 12, further comprising an alert

2   processing system that tracks inputted alert indications, filters

3   out inputted alert indications that do not meet a threshold

4   value, compares the inputted information to a tracking rule to

5   determine whether the inputted information should be associated

6   with a declared incident.

1   20. The system of claim 19, wherein the enterprise is a

2   network, and the inputted information is supplied by a number of

3   network devices.

1   21. The method of claim 3, comprising updating the incident

2   ticket based an updated tracking rule such that the alert

3   indications, conclusions and description reflect the updated

4   tracking rule.

1   22. The method of claim 21, wherein the tracking rule is

2 updated using human input based on observations of reported

3 incidents.

1